**UNITED STATES DISTRCIT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**

| | |
|---|---|
| ERIN MINOR, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>SET FORTH, INC.<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Erin Minor ("Plaintiff"), individually and on behalf of others similarly situated (the "Class" or "Class members"), hereby brings this class action complaint against Defendant, Set Forth, Inc ("Defendant"). Plaintiff alleges as follows upon personal knowledge as to her own acts and experiences, and upon the investigation of her attorneys as to all other matters.

## INTRODUCTION

1. This is a data breach class action on behalf of individuals whose personally identifying information ("PII") was stolen by cybercriminals as part of a major cyber-attack on Defendant's systems. It was reported that on or about May 21, 2024, there was unauthorized access to Plaintiff's and many other individuals' PII (the "Data Breach").[1] Information compromised in the breach included full names, addresses, dates of birth, and Social Security

[1] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html.

numbers (SSNs).[2] Over 1.5 million customers' information was included in the data breach, according to Defendant's notice to affected customers.[3]

2. Defendant is a privately-held corporation incorporated in Delaware with its principal place of business in Illinois. Defendant is a "dedicated account administrator and processor for consumers enrolled in a debt relief program."[4] It provides consumers with online access to view account balances, settlement information, and other financial wellness tools.[5]

3. Plaintiff brings this lawsuit on behalf of herself and others similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information was likely accessed by an unknown third party and precisely what specific type of information was accessed.

4. By taking possession and control of sensitive information such as PII, Defendant assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' PII from unauthorized disclosure.

5. Defendant also has a duty to adequately safeguard individuals' sensitive and private information under industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"), and other relevant laws and regulations.

6. Defendant breached its duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect individuals' PII from unauthorized access and disclosure.

---

[2] Notice of Data Breach, https://www.setforth.com/notice-of-data-security-incident/.
[3] *Id.*
[4] https://www.setforth.com/consumers/.
[5] *Id.*

7. Defendant has offered no assurance that the sensitive and private information that was accessed in the Data Breach has been recovered or destroyed.

8. The exposure of a person's PII through a data breach substantially increases that person's risk of identity theft, fraud, and similar forms of criminal mischief, potentially for the rest of their lives. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts and email accounts. Mitigation of the risk of misuse of their sensitive and private information may not even be possible.

9. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. Plaintiff and Class members are now at a substantially increased risk of experiencing misuse of their PII in the coming years. This action seeks to remedy these failings and their consequences.

10. The injury to Plaintiff and Class members is compounded by the fact that Defendant has yet to notify the victims of its occurrence. Defendant's failure to timely notify the victims of the Data Breach meant that Plaintiff and Class members were unable to take premature measures to prevent or mitigate the resulting harm.

11. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was stolen in the Data Breach. Plaintiff asserts claims for negligence, breach of implied contract, unjust enrichment, and violation of Illinois consumer protection laws, and seeks declaratory relief, injunctive relief, monetary damages, punitive damages, equitable relief, and all other relief authorized by law.

## PARTIES

**Plaintiff**

12. Plaintiff Erin Minor is an adult residing in Austell, Georgia. Plaintiff received A

breach notice letter from Defendant stating that her personal information was compromised in the Data Breach.

**Defendant**

13. Defendant Set Forth, Inc., is a Delaware corporation with a principal place of business at 1900 E Golf Rd., Suite 550, Schaumburg, IL 60173.

## JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million dollars, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Defendant. See 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

15. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District, regularly conducts business in this District, and the acts and omissions giving rise to Plaintiff's claims emanated from within this District.

16. Venue is proper under 18 U.S.C. § 1391(b) because Defendant maintains its principal place of business in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

## FACTUAL ALLEGATIONS

***The Data Breach***

17. Defendant claims that on May 21, 2024, it discovered suspicious activity from an unauthorized user on its systems and determined on July 1, 2024 that the unauthorized user had gained access to documents in its system. On information and belief, the type of information that Defendant maintains includes, *inter alia*: full names, addresses, dates of birth, and Social Security numbers (SSNs).

18. On information and belief, as Defendant has not stated otherwise, Plaintiff's and Class Members' PII is still in the possession of the cybercriminals, nearly six months after Defendant identified the unauthorized user on its systems.

19. Due to the highly sensitive nature of the information Defendant collects and maintains, Defendant is obligated provide confidentiality and adequate security for individuals information in compliance with statutory privacy requirements and industry standards.

20. Upon information and belief, Plaintiff and Class Members may have provided their PII, including their SSNs, to Defendant.

21. Plaintiff and Class Members received notice beginning on or about November 8, 2024, that their information which was in Defendant's possession was accessed in the Data Breach.

22. The notices received by Plaintiff and Class members specifically mention that their data was compromised in the Data Breach.

23. Plaintiff and Class Members are entitled to protections to keep their sensitive PII, including their social security numbers, confidential and secured, to use such information for business purposes only, and to make only authorized disclosures of this information.

24. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to malicious third parties.

25. Defendant failed to employ reasonable security practices and procedures appropriate to protect the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII to an unauthorized third party.

26. As evidenced by the Data Breach's occurrence, the PII contained on Defendant's systems was not encrypted. Had it been, the data thieves would have stolen only unintelligible data.

27. Plaintiff and Class members now live with their PII exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

28. Plaintiff and Class members now face constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages, in addition to any fraudulent use of their PII.

***Defendant Knew that Criminals Target Valuable PII and Failed to Take Action to Prevent Theft***

29. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, Defendant's systems would be attractive for cybercriminals.

30. On May 21, 2024, Set Forth, Inc. detected that its systems had been infiltrated by an unauthorized user. Nearly two weeks later, Defendant determined that the unauthorized user had gotten access to documents related to its users containing PII.

31. Defendant knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

32. The risks are not theoretical. The prevalence of data breaches has increased dramatically over the years: "The number of reported data breaches in the U.S. rose to a record 3,205 in 2023, up 78% from 2022 and 72% from the previous high-water mark in 2021, according to the nonprofit Identity Theft Resource Center."[6]

33. In recent years, numerous high-profile breaches have occurred including breaches

[6] Stuart Madnick, *If Companies Are So Focused on Cybersecurity, Why Are Data Breaches Still Rising?*, THE WALL STREET JOURNAL (Mar. 15, 2024), https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c (last visited Oct. 20, 2024).

involving MoveIt, First American Financial Corp., JP Morgan Chase & Co., and Equifax.

34. In tandem with the increase in data breaches, the rate of identity theft has increased. Since 2019, identity theft reports have increased $68.3%. In the second quarter of 2023, roughly 277,620 ID theft reports were submitted to the Federal Tarde Commission, which was a substantial increase from the 164,982 reported in the same quarter in 2019.[7]

35. Every state has experienced an increase in identity theft over 11% per 100,000 residents since 2019.[8]

36. PII has considerable value to hackers. Hackers sell stolen data on the black market through the "proliferation of open and anonymous cybercrime forums on the Dark Web that serves as a bustling marketplace for such commerce."[9]

37. The breadth of data that can be bought and sold leaves Defendant's consumers especially vulnerable to identity theft, tax fraud, credit and bank fraud.

38. Consumers also place a high value on the privacy of their data. Studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

39. Recently, more consumers are exercising their Data Subject Access Rights and

---

[7] Julie Ryan Evans, *93 of 100 Largest US Metros and All States Hae Seen Increase in ID Theft Reports Since 2019*, LENDINGTREE (Nov. 6, 2023), https://www.lendingtree.com/insurance/id-theft-study/#:~:text=Identity%20theft%20reports%20have%20increased,the%20same%20quarter%20in%202019 (last visited Oct. 20, 2024).

[8] *Id.*

[9] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Oct. 20, 2024).

[10] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

leaving providers over their data practices and policies.[11]

40. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

41. Defendant certainly knew and understood that unprotected or exposed PII in its custody is highly valuable and sought after by nefarious criminals seeking to illegally monetize that PII through unauthorized access.

42. Armed with this knowledge, Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' PII from being stolen.

***Plaintiff Erin Minor's Experience in the Data Breach***

43. On November 12, 2024, Plaintiff received a notification letter from Defendant informing her about the Data Breach and that her personal information was compromised.

44. Upon information and belief, Plaintiff's PII was exposed and accessed in the Data Breach.

45. On or around November 12, 2024, Plaintiff also received notice about a credit inquiry received on her credit report. She has not opened any new financial accounts in recent weeks.

46. As a result, Plaintiff has had to spend time and resources monitoring her credit report and financial accounts for fraudulent activity.

47. Plaintiff is careful about sharing her private information. Plaintiff stores any

[11] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742

documents containing private information in a safe and secure location. She never knowingly transmitted unencrypted private information over the internet or any other unsecured medium. Plaintiff would not have entrusted his private information with Defendant had she known of Defendant's failure to implement and maintain data security measures.

48. Defendant continues to maintain Plaintiff's PII and has a legal obligation to protect that PII from being compromised or exposed by unauthorized users.

49. Plaintiff is now at a substantial risk of identity theft and will spend future time and resources to monitor her accounts and mitigate the risk of identity theft and/or other types of fraud.

***Defendant Failed to Comply with the FTCA and FTC Guidelines***

50. The Federal Trade Commission Act ("FTCA") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45.

51. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which reflect the importance of implementing reasonable data security practices.

52. The FTC's publication, Protecting Personal Information, established cyber-security guidelines for businesses. The guidelines provide that businesses should take action to protect the personal information that they collect; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[12]

53. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the

[12] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

system; and have a response plan ready in the event of a breach.[13]

54. The FTC further recommends that businesses not maintain private information longer than is needed for authorization of a transaction; limit access to sensitive information; require complex passwords be used on networks; use industry-tested methods for security monitor for suspicious activity on the networks; and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII adequately and reasonably under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

56. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendant failed to properly implement basic data security practices.

58. Defendant was at all relevant times fully aware of its obligations to protect individuals' PII, and of the significant consequences that would result from its failure to do so.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Consequently, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach and causing injury to Plaintiff and Class members.

***Defendant Failed to Comply with Industry Standards***

61. Entities like Defendant are particularly vulnerable to cyberattacks because of the sensitive nature of the information that they collect and maintain.

[13] *Id.*

62. Due to this vulnerability, there are industry best practices that should be implemented by entities like Defendant.

63. These practices include but are not limited to: Educating and training employees about the risks of cyberattacks, strong passwords, multi-layer security such as firewalls, anti-virus and malware software, encryption, multi-factor authentication, backup data, limitation of employees with access to sensitive data, setting up network firewalls, switches and routers, monitoring and limiting the network ports, and monitoring and limited access to physical security systems.

64. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

65. The Defendant's failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiff and Class Members.

***Common Damages Sustained by Plaintiff and Class Members***

66. For the reasons mentioned above, Plaintiff and all other Class Members have suffered injury and damages directly attributable to Defendant's failure to implement and maintain adequate security measures, including, but not limited to: (i) fraudulent credit card applications attempted in their name (ii) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) invasion of

their privacy; (vi) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face

## CLASS ALLEGATIONS

67. Plaintiff brings this class action individually and on behalf of all persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

68. Plaintiff seeks certification of a Class as defined below and subject to further amendment:

> **Nationwide Class**
>
> All individuals in the United States whose PII was compromised in the Data Breach (the "Class").
>
> **State Subclass**
>
> All individuals residing in Georgia whose PII was compromised in the Data Breach (the "Georgia Subclass").

69. Excluded from the Class is Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

70. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

71. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Defendant disclosed that the personal information of 1.5 million consumers was compromised in the Data Breach. The number of individuals and contact information of those individuals are available from Defendant's business records. Thus the Class is sufficiently numerous.

72. Commonality. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure;
- Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;
- Whether Defendant breached its duties to protect Plaintiff's and Class members' PII;
- When Defendant learned of the Data Breach;
- Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;
- Whether hackers obtained Plaintiff's and Class members' data in the Data Breach;
- Whether an implied contract existed between Plaintiff, Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure;
- Whether Defendant was unjustly enriched;
- Whether Plaintiff and Class members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and
- Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

73. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

74. Adequacy of Representation. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that they have no interests adverse to, or in conflict with, the Class they seek to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

75. Superiority. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

76. All members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class members affected by the Data Breach.

77. Finally, class certification is appropriate under Fed. R. Civ. P. 23(b). Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
### (Plaintiff, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)

78. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

79. Defendant requires that its consumers, including Plaintiff and Class members, submit private information such as PII in the course of providing its services.

80. Defendant collected, acquired, and stored Plaintiff's and Class members' private information on its servers.

81. Plaintiff and Class members entrusted Defendant with their private information and had the understanding that Defendant would safeguard their information.

82. Defendant had knowledge of the sensitivity of Plaintiff's and Class members' private information, and the consequences that would result from the unauthorized disclosure of such information. Defendant knew that entities similar to itself have been the target of cyber-attacks in the past, and that Plaintiff and Class members were the foreseeable and probable victims of any inadequate data security procedures.

83. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to Plaintiff and Class members.

84. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their private information in its possession, custody, or control from the unauthorized disclosure of such information.

85. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the FTCA, and industry standards.

86. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

87. Upon information and belief, the PII of Plaintiff and Class members was disclosed to unauthorized third persons as a result of the Data Breach. Further, Plaintiff and Class members have received notice from credit and identity monitoring services that their PII was found on the dark web because of the Data Beach.

88. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members caused their PII to be compromised in the Data Breach.

89. Plaintiff and Class members were in no position to protect their PII themselves.

90. But for Defendant's breach of the duties described herein, Plaintiff and Class members' PII would not have been compromised.

91. There is a causal relationship between Defendant's failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect the PII of individuals and the harm suffered by Plaintiff and Class members.

92. As a direct and proximate result of Defendant's conduct described above, it directly and proximately caused the Data Breach, and Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v)

deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

93. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

94. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

95. Defendant's negligent conduct is ongoing, in that it still holds Plaintiff's and Class members PII in an unsafe and insecure manner.

96. Plaintiff and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class members.

## COUNT II
## NEGLIGENCE *PER SE*
**(Plaintiff, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)**

97. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

98. Defendant' duties arise from, *inter alia*, Section 5 of the FTCA.

99. Defendant violated Section 5 of the FTCA by failing to implement reasonable security measures to Protect Plaintiff's and Class members' PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving

PII including, specifically, the substantial damages that would result to Plaintiff and Class members.

100. Defendant's violations of Section 5 of the FTCA constitutes negligence *per se*.

101. Plaintiff and class members are within the class of persons that Section 5 of the FTCA was intended to protect.

102. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA was intended to guard against.

103. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit reasonable data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

104. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

105. As a direct and proximate result of Defendant's violations, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

106. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

107. Plaintiff and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen their data security procedures and to provide credit monitoring to Plaintiff and Class members.

## COUNT III
## BREACH OF IMPLIED CONTRACT
**(Plaintiff, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)**

108. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

109. In connection with receiving services from Defendant, Plaintiff and all other Class members entered into implied contracts with Defendant or were intended third-party beneficiaries of contracts between Defendant and others.

110. Pursuant to these implied contracts, money was paid to Defendant, whether directly from Plaintiff and Class members or indirectly, and Defendant stored the PII of Plaintiff and Class members on its network. In exchange, Defendant impliedly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

111. The protection of PII was a material term of the implied contracts that were either between Plaintiff and Class members, on the one hand, and Defendant, on the other hand or were

between third parties and Defendant to which Plaintiff and Class members were intended third party beneficiaries.

112. Plaintiff and Class members or the third parties fulfilled their obligations under the contracts.

113. Defendant breached its obligations by failing to implement and maintain reasonable data security measures to protect and secure the PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

114. Defendant's breach of its obligations of its implied contracts directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

115. Plaintiff and all other Class members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII has been breached; (vi) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

## COUNT IV
## UNJUST ENRICHMENT
**(Plaintiff, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)**

116. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully

set forth herein.

117. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim (Count III)

118. Plaintiff and Class members have an interest, both equitable and legal, in the private information about them that was collected, secured, and maintained by Defendant and that was ultimately compromised in the Data Breach.

119. A financial benefit was conferred upon Defendant when Plaintiff and Class members provided their PII, including their social security numbers to Defendant. Defendant's business model would not exist save for the need to ensure the security of Plaintiff's and class members' private information.

120. The relationship between Defendant, Plaintiff and Class members is not attenuated, as Plaintiff and Class members had a reasonable expectation that the security of their information would be maintained when they provided their information to Defendant, or when Defendant otherwise took control of their information. Plaintiff and Class members were induced to provide their information in reliance on the fact that Defendant's data security measures were adequate.

121. Upon information and belief, this financial benefit was, in part, conferred when portions of Plaintiff and Class members' information were used by Defendant to obtain payments from other consumers for access to Defendant's database of personal information containing Plaintiff's and Class member's PII, including their social security numbers.

122. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members by acquiring and/or collecting their private information as a necessary part of obtaining Defendant's services. Defendant appreciated and benefitted from the receipt of Plaintiff's and Class members' private information in that they used the private information and

profited from the transactions in furtherance of its business.

123. Defendant also understood and appreciated that the PII pertaining to Plaintiff and Class members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

124. Defendant acquired Plaintiff's and Class members' private information through inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

125. As a result of Defendant's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

126. Defendant should not be permitted to retain the payments which include information belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal and state law and industry standards.

127. Defendant unjustly enriched itself by using payments containing private information provided by Plaintiff and Class members to further its business.

128. Notably, Defendant chose not to use any payments received to enhance their data security procedures.

129. Under principles of equity and good conscience, Defendant should not be permitted to retain the payments wrongfully obtained from Plaintiff and Class members, and be compelled to provide for the benefit of Plaintiff and Class members, all unlawful proceeds received by it as a

result of the conduct and Data Breach alleged herein.

**COUNT V**
**VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT, O.C.G.A. §§ 10-1-912, *et seq.***
**(Plaintiff, individually and on behalf of the State Subclass)**

130. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

131. Defendant is a business that collects and maintains information includes Personal Information as defined by O.C.G.A. § 10-1-912(a).

132. Plaintiff and Georgia Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered under O.C.G.A. § 10-1-912(a).

133. Defendantis required to accurately notify Plaintiff and Georgia Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

134. Because Defendant was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Personal Information, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by O.C.G.A § 10-1-912(a).

135. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated O.C.G.A. § 10-1-912(a).

136. As a direct and proximate result of Defendant's violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

137. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912 including actual damages and injunctive relief.

**COUNT VI**
**VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT, O.C.G.A. §§ 10-1-370, *et seq.***
**(Plaintiff, individually and on behalf of the State Subclass)**

138. Plaintiff realleges and incorporates by reference all preceding paragraphs as if set fully herein.

139. Defendant, Plaintiff, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

140. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including: Representing that goods or services have characteristics that they do not have; Representing that goods or services are of a particular standard, quality, or grade if they are of another; Advertising goods or services with intent not to sell them as advertised; and Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

141. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' Personal Information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C.

142. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

143. Defendant intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

144. In the course of its business, Defendant engaged in activities with a tendency or capacity to deceive.

145. Defendant acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass members' rights.

146. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue

in business and it would have been forced to adopt reasonable data security measures and comply with the law.

147. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

148. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

## COUNT VII
## DECLARATORY JUDGMENT
**(Plaintiff, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)**

149. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth here.

150. As previously alleged, Plaintiff and Class members were third party beneficiaries of contracts that required Defendant to provide adequate security for the PII it collected. As previously alleged, Defendant owes duties of care to Plaintiff and Class members that require it to adequately secure customer data.

151. Defendant still possesses customer data pertaining to Plaintiff and Class members.

152. Defendant has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems.

153. Accordingly, Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Defendant's lax approach towards data security has become public, the PII data in its possession is more vulnerable than

previously.

154. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

155. Plaintiff, therefore, seeks a declaration that (a) Defendant's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant systems;

e. purging, deleting, and destroying in a reasonable secure manner customer data not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps Defendant customers must take to protect themselves.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

## JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 18, 2024

Respectfully submitted,

By: */s/ Katrina Carroll*
Katrina Carroll
katrina@lcllp.com
**LYNCH CARPENTER LLP**
111 W. Washington Street
Suite 1240
Chicago, IL 60602
Telephone: 312-750-1265

Beena M. McDonald*
bmm@chimicles.com
Samantha Barrett*
sb@chimicles.com
Mariah Heinzerling*
mh@chimicles.com
**CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP**
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

**pro hac vice* to be submitted

*Counsel for Plaintiff and the Proposed Class*